科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１９　日現在

機関番号：　３２６４１
研究種目：　挑戦的萌芽研究
研究期間：　2013～2013
課題番号：　２５５４００４９

研究課題名（和文）耐タンパデバイスを利用した効率的な関数型暗号設計法および安全性検証法の研究

研究課題名（英文）A research on designing efficient and secure functional encryption schemes with tamper-proof devices

研究代表者
今井　秀樹（Imai, Hideki）

中央大学・理工学部・教授

研究者番号：７００１７９８７

交付決定額（研究期間全体）：（直接経費）　　2,900,000円、（間接経費）　　870,000円

研究成果の概要（和文）：近年，ネットワークサービスからの情報漏洩問題が大きな社会問題となっており，その根本的解決手法の確立が求められている．本研究では，この問題に対処するために関数型暗号を応用した安全なアクセス制御方式の実現を目的とし，関数型暗号の実用化に必要となる基盤技術の研究開発を行った．本研究の研究成果として以下の２点が得られた．(1)関数型暗号を効率よく実装するための一つの方法として，耐タンパデバイスの部分的利用が有効であると考え，暗号実装の一部を耐タンパデバイス上で実施する際の安全性評価を行った．(2)関数型暗号自体の鍵漏洩対策として，復号鍵の更新が可能な効率的な関数型暗号を提案し，その安全性評価を行った．

研究成果の概要（英文）：Data leakage from network services has been a serious problem in our society. To overcome this problem, functional encryption schemes can be used. Functional encryption schemes realize an access control mechanism over encrypted data. However, functional encryption schemes are not yet in practical use due to the long key lengths, and their high encryption/decryption costs. In this research, we develop fundamental techniques to realize high performance functional encryption schemes using tamper-proof devices. We also give a security evaluation on cryptographic tamper-proof devices.

研究分野：　情報学

科研費の分科・細目：　計算基盤・情報セキュリティ

キーワード：　暗号理論　耐タンパデバイス　物理解析攻撃

１．研究開始当初の背景

情報機器やコンピュータネットワークの発展により，様々なネットワークサービスが広く普及し，我々の生活に不可欠な社会インフラの一つとなっている．しかしながら，サイバー攻撃などによるネットワークサービスからの情報漏洩事故は跡を絶たず，大きな社会問題となっている．これまで多くの情報漏洩対策手法が提案されているが，それらの多くは対症療法的な手法であり，情報漏洩を原理的に防止できる手法は現時点においては存在しない．そのため，情報漏洩問題の根本的解決技術の確立は社会的に重要な研究課題となっている．

ネットワークサービスにおける主要なサービスの一つとして，利用者が低価格で大容量のストレージを利用することができるオンラインストレージサービスがあり，広く利用されている．オンラインストレージサービスにおける情報漏洩問題解決策として，サーバ上では全ての情報を暗号化しておき，暗号文のままアクセス制御等を行う方式が考えられる．こうすることで，サーバ上では，暗号文を復号する必要がなくなるため，万が一サーバから何らかの情報が漏洩したとしても，暗号文であるため安全性が確保される．このような暗号文に対するアクセス制御を実現する暗号方式は関数型暗号と呼ばれる．関数型暗号では，暗号化の際に復号できる条件（アクセスポリシー）を暗号化鍵として利用する．また復号鍵には，属性と呼ばれる情報の集合が割り当てられる．復号鍵に割り当てられた属性の集合が，暗号文に割り当てられたアクセスポリシーを満たす場合に限り，暗号文はその復号鍵を用いて復号することができる．このメカニズムを利用することで，サーバ上で暗号文の復号を行うことなく，アクセス制御を実現している．

関数型暗号は，2005 年にサハイ(A. Sahai)らによるファジーID ベース暗号の提案以来，活発に研究が行われてきた．これまでに提案された関数型暗号として，鍵ポリシー属性ベース暗号，暗号文ポリシー属性ベース暗号，内積述語暗号などの方式がある．しかしながら，現在のところ関数型暗号は実用化には至っていない．

２．研究の目的

本研究の目的は，ネットワークサービスからの情報漏洩問題の根本的解決を目指し，そのために必要な関数型暗号の実用化に向けた基盤技術の研究開発を行うことである．

関数型暗号は，暗号文に対するアクセス制御機構を備え，ネットワークサービスに適した暗号方式である．しかしながら，関数型暗号は現在の段階では実用化には至っていない．その理由として，関数型暗号では鍵のサイズが利用する属性の個数に応じて変化するために，公開鍵暗号などと比較して鍵のサイズが非常に大きくなることや，暗号化・復号においてペアリングと呼ばれる楕円曲線上で定義される関数の演算が必要となることにより計算コストが大きくなることが考えられる．本研究では，関数型暗号の実用化に向けて，これらの問題に対する解決法に関する研究を行い，関数型暗号の実用化に貢献する．

３．研究の方法

本研究では，関数型暗号の実用化に向けた研究として以下の 2 つの方向から研究を実施した．

(1)関数型暗号の暗号化・復号処理を高速に処理するために，暗号の一部の演算を専用のハードウェア上で実装する方式を提案し，その安全性に関する評価を行う．

物理デバイス上に実装した暗号回路では，そのデバイスの実行時の消費電力量や漏洩電磁波などが回路内の秘密情報と相関を持つことが知られており，実際に消費電力等をオシロスコープを利用して多数取得し，統計処理を行うことで，秘密情報を特定できることが知られている．このような攻撃はサイドチャネル攻撃と呼ばれ，オシロスコープと PC があれば低コストで容易に実行できることから，大きな脅威となっている．そのため，暗号アルゴリズムを物理デバイス上に実装する際にはサイドチャネル攻撃に対し十分な耐性を持つようにすることが求められる．

本研究では、関数型暗号の暗号化・復号処理の高速化のために，これらの処理の一部を専用の物理デバイスで行う状況を想定し，その安全性を評価する．

(2)関数型暗号の復号鍵の漏洩対策手法の研究を行う．

関数型暗号を実用化するにあたり，利用者が持つ復号鍵の漏洩対策が必要である．一般に，暗号方式が物理デバイスを含めどれだけ高い安全性を持っていたとしても，利用者が持つ復号鍵が漏洩した場合，その暗号方式の安全性は失われる．一度鍵の漏洩が発生した場合，即座に鍵の再発行を行ったとしても，過去に通信された暗号文は全て漏洩した鍵を利用して復号が可能となってしまう．本研究では，復号鍵を時刻に対応付けて更新できる関数型暗号方式を提案することで，復号鍵漏洩問題の解決を目指す．

４．研究成果

本研究の主な研究成果は以下のとおりである．

(1) **暗号化・復号処理を行う物理デバイスの安全性評価**

サイドチャネル攻撃に関する過去の研究成果から，AES に対してサイドチャネル攻撃

を成功させるためには，回路の実装方式にもよるが，数千から数万の消費電力波形が必要となることが明らかになっている．しかしながら，攻撃者の消費電力波形取得能力を現実的に考えると，数千から数万の消費電力波形を取得することは困難であることも多い．その理由として，デバイス内に保持されている秘密鍵は永続的に同じものが利用されることは少なく，定期的に更新されることが多いことなどが挙げられる．このような状況において，攻撃者が数千以上もの消費電力波形を得ることは困難であり，数十～百程度の波形しか取得できないこともあると考えられる．攻撃者が十分な数の波形を取得できなかった場合，サイドチャネル攻撃による鍵の完全特定は困難であると考えられるが，鍵の部分情報は特定される可能性は否定できない．したがって，攻撃者が少数の消費電力波形からサイドチャネル攻撃によって得た鍵の部分情報を利用して，最終的に鍵全体を完全に特定するために必要となる計算量を評価することは，サイドチャネル攻撃に対するデバイスの安全性を評価する上で重要となる．

本研究では，攻撃者がサイドチャネル攻撃を成功させるために必要な数の消費電力波形を得られない状況において，攻撃者が鍵全体を復元するために必要となる計算量を見積もることで，現実的なサイドチャネル攻撃の脅威を評価した．提案手法では，通常の相関電力解析法(Correlation Power Analysis, CPA)に加え，暗号鍵のバイト位置毎にレジスタ内容と消費電力との相関値の特性を解析することで，CPA で得た鍵の部分情報から効率よく鍵全体を復元する手法を提案した．

サイドチャネル攻撃では，一般に暗号鍵に対してバイト毎に独立に総当り探索を行い，バイト毎に最も正解鍵に近いと考えられるものを見つけ出す戦略を取る．相関電力解析においては，デバイス内のレジスタの状態遷移量と消費電力が線形相関を持つという性質を利用し，バイト毎の全鍵候補に対して，鍵に依存するレジスタの状態遷移量と消費電力との相関係数を求め，最も高い相関値を得た鍵候補を真の鍵と特定する．もし，攻撃者が十分な個数の波形数を得られなかった場合，真の鍵の持つ相関係数値が全鍵候補中で一位とならず二位以下となり，攻撃は失敗すると予想されるが，このような場合であっても，鍵のバイト位置や回路の構造などにより，正解鍵が相対的に高い相関値を取る可能性がある．本研究ではまず，この事実を検証するためにサイドチャネル攻撃標準評価ボード SASEBO-GⅡを用いて検証実験を行った．実験の結果，AES-128 の鍵 16 バイトの中で平均 9 個のバイト位置において，正解鍵の相関係数が 256 個の候補鍵中上位 32 位以内に入ることが明らかになった．しかし，全てのバイト位置で正解鍵が高い相関係数を持つわけではなく，バイト位置により正解鍵の相関係数の値に偏りがあることも明らかになった．この鍵のバイト位置による相関係数値の偏りを利用し，効率よい鍵の完全特定法を提案し，その計算量を評価した．評価のために，SASEBO-GⅡを利用し実験を行った．実験では，SASEBO-GⅡ上の FPGA チップに実装された AES の消費電力波形を 1,000 個取得し，それらの波形を利用して提案手法を用いた攻撃実験を行い，鍵の完全復元に必要となる計算量を特定した．実験による評価の結果，鍵の完全特定のためには，およそ 2^{90}～2^{110} 程度の計算量が必要となることが分かった．

本実験結果より，サイドチャネル攻撃は強力な攻撃ではあるが，攻撃に十分な個数の波形を攻撃者が取得できない場合においては，攻撃者は現実的な時間内において鍵の復元は不可能であることが示された．

本研究のもう一つの成果である鍵の更新機能を持つ関数型暗号方式をハードウェア上に実装し，利用する場合，鍵は定期的に更新されるため攻撃者が同じ鍵の波形を多数取得することはさらに困難になる．このことから，秘密鍵の定期的な更新は，鍵の漏洩対策だけではなく暗号方式を物理デバイス上で実行する際に，有効な安全対策手法となり得ると言える．

(2)関数型暗号に対する鍵漏洩対策手法の開発

関数型暗号に限らず，暗号方式を安全に利用するためには，秘密鍵を機密に保持する必要がある．たとえどれだけ安全な暗号方式であっても，秘密鍵が一度漏洩してしまうと，暗号の安全性は失われる．秘密鍵を安全に保持することは，極めて重要な事柄であるが，ユーザの操作ミスやマルウェア感染などによって秘密鍵が意図せず漏洩してしまうことは現実に少なくない．

関数型暗号では，一つの暗号文を復号できる鍵は一つとは限らない．暗号文に付加されたアクセスポリシーを満たす鍵ならばどの鍵でも暗号文が復号できる．したがって，関数型暗号においては一つの鍵が漏洩すると，そのユーザ向けの暗号文だけではなく，他のユーザのための暗号文も不正に復号される可能性がある．このような理由から，関数型暗号の実用化のためには，鍵の漏洩対策機構が暗号方式に組み込まれていることが望ましい．

関数型暗号における鍵の漏洩対策技術としては，これまでに鍵失効機能付き属性ベース暗号が提案されている．鍵失効機能付き暗号では，ある鍵が漏洩した場合，その鍵を失効させることで，以降その鍵を用いた復号ができなくなる．その一方で，失効以前に暗号

化されていた暗号文は，失効した鍵による復号が可能であるため，鍵の失効機能だけでは鍵の漏洩による被害を完全に防ぐことはできない．本研究では，鍵が漏洩した場合に，漏洩以前に暗号化された暗号文を保護する方式を提案する．提案手法と，鍵失効機能を組合せて利用することで，関数型暗号における有効な鍵漏洩対策が実現可能となる．

本研究では，以下の様な機能を持つ関数型暗号を設計する．まず，平文を暗号化する際に，暗号化鍵となるアクセスポリシーと共に現在時刻を入力し暗号化を行う．復号鍵の生成は，既存の関数型暗号と同じく信頼できる鍵生成局が行う．鍵生成局は，各ユーザに対し，ユーザの持つ属性集合と時刻 0 に対応する復号鍵を発行する．復号を行うユーザは，復号鍵に関連付けられた時刻を更新し，現在時刻に対応した復号鍵を自身で生成することができる．ただし，鍵の更新時には鍵に関連付けられた属性集合は変わらないようにする．また,鍵の更新と同時に，ユーザは古い鍵を廃棄する．さらに，ユーザ自身で鍵の更新が可能である一方で，新しい鍵から古い鍵を生成することは計算量的に困難となるように設計する．暗号文の復号は，暗号文に関連付けられたアクセスポリシーを鍵が満たし，かつ暗号文と鍵に付加された時刻情報が一致した場合にのみ可能となる．この鍵更新機能を実現することで，万が一ある時刻において復号鍵が漏洩したとしても，その時刻より以前に暗号化された暗号文は復号することができない．

本研究では，上記の機能を持つ関数型暗号を実現するために，2010 年にウォータース(B. Waters)らによって提案された暗号文ポリシー型属性ベース暗号と呼ばれる関数型暗号方式を元に，復号鍵の更新機能を付加した方式を提案した．さらに，鍵更新機能付きの属性ベース暗号に対し，最も高い安全性と考えられる，選択暗号文攻撃に対する識別不可能性と呼ばれる安全性を定式化し，提案手法がこの安全性を満たすことを数学的に証明した．安全性の証明には Dual System Encryption と呼ばれる安全性証明手法を利用し,三つの計算量問題に帰着することで証明を行った．

本方式が提案されるまで,選択暗号文攻撃者に対する安全性を持つ,鍵の漏洩対策機能付きの属性ベース暗号は存在しなかった.提案手法により,属性ベース暗号の実用化に必須である鍵の漏洩対策機能が実現された．

５．主な発表論文等

〔雑誌論文〕（計　1 件）

[1] Takashi Kitagawa, Hiroki Kojima, Nuttapong Attrapadung, and Hideki Imai, “Efficient and Fully Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption,” Information Security, Lecture Notes in Computer Science, 2014. (査読有)

〔学会発表〕（計 5 件）

[1] 柳島佳衣斗，北川隆，ミハイエビッチ・ミオドラッグ，今井秀樹，“CPA 攻撃結果から鍵を完全特定するために要する計算量の考察,”2014 年暗号と情報セキュリティシンポジウム，2014 年 1 月，鹿児島県鹿児島市．

[2] 早崎拓馬，山口利恵，今井秀樹,“第三者 Cookie を用いた Web 履歴のプライバシー問題について，”2014 年暗号と情報セキュリティシンポジウム，2014 年 1 月，鹿児島県鹿児島市．

[3] 細谷玲奈，北川隆，ミハイエビッチ・ミオドラッグ，古原和邦，今井秀樹，“Niederreiter 暗号に基づく新たな軽量化認証プロトコル，”2014 年暗号と情報セキュリティシンポジウム，2014 年 1 月，鹿児島県鹿児島市．

[4] 鈴木隆明，山口利恵，今井秀樹，“パーミッションを用いた不正動作アプリケーションの現状調査と検出方法，”2014 年暗号と情報セキュリティシンポジウム，2014 年 1 月，鹿児島県鹿児島市．

[5] 恩田 泰則，辛 星漢，古原 和邦，今井秀樹，“Strong Diffie-Hellman Problem を難しくする群位数の選び方に関する考察,”2014 年暗号と情報セキュリティシンポジウム，2014 年 1 月，鹿児島県鹿児島市．

６．研究組織

(1)研究代表者

今井　秀樹　（IMAI, Hideki）
中央大学　理工学部　教授
研究者番号：70017987